Office of State Controller, and the North Carolina Department of the Secretary of State, and North Carolina Department of Cultural Resources, Division of Archives and Records

DocuSign® How-to Guide

Version 1.0

June 2013

DocuSign® How-to Guide

Table of Contents

1 Introduction

1.1 Purpose of How-To Guide on DocuSign®

This document serves as a how-to guide for the use of DocuSign® e-signature platform. This guide is specific to the vendor product, DocuSign®. For general guidelines on electronic signature (e-signatures) see the Best Practices Guide on Electronic Signatures located www.ncdcr.gov/archives. This how-to guide provides information on the following:

- E-signature background
- Introduction to DocuSign®
- DocuSign® Contract Specifics
- DocuSign® Account Administration
- Digital Signature and Electronic Records Management
- Additional Resources

2 E-Signature Background

2.1 State Legislation on Acquiring an E-Signature Platform

E-signatures allow for secure online document signing. An e-signature authenticates the identity of the signer of a document and it ensures that the original content of the signed document is unchanged. Under the North Carolina Uniform Electronics Act (UETA), e-signatures are legally-binding.

North Carolina session law 2011-145, House Bill 200 6A.18, effective October 1, 2011, gave the state Office of State Controller the task of planning, developing, and implementing "a coordinated enterprise electronic forms and digital signatures capabilities. In developing this capability, the State Controller shall determine the cost of converting forms to an electronic format, determine priorities for converting forms, and establish milestones for completing this conversion." The State Controller's office formed a workgroup to establish requirements for implementing a digital signature management system and investigate potential providers. Representatives from nine different agencies – DOJ, DOT, DOR, DPS, AOC, DHHS, Sec. of State, Cultural Resources, Industrial Commission— participate in the Authentication Workgroup. The workgroup created specifications for the Request of Proposal and met with several vendors to assess how their products met the ROP's criteria. In the end, the State entered into a 2-year contract with DocuSign®.

2.2 Definitions

API (Application Program Interface): The Society of American Archivists defines an API as "software conventions that provide a link between one application and another piece of software. APIs are used primarily to support portability of applications across different operating systems. A single application makes calls to APIs customized to support that application on different platforms."[1]

[1] "A Glossary of Archival and Records Terminology." Society of American Archivists

Authentication: Authentication is the process of verifying a document or record is genuine or original. In the case of electronic documents, it is the process of confirming a user's identity.

Cloud Computing: The National Institute of Standards and Technology (NIST) defines cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[2]

Digital Signatures: A complex string of electronic data that is embedded in an electronic document for the purposes of verifying document integrity and signer identity.[3]

Electronic Signatures: An electronic sound, symbol, or process attached to, or logically associated with, a record and executed or adopted by a person with the intent to sign the record.[4]

Envelope: A DocuSign® envelope is an electronic record containing one or more document consisting of a single page or a group of pages of data uploaded to the System.

Encryption: A data security method that translates transferred data into a secret code that can only be decrypted by providing a password or other private key indicator.

Metadata: Metadata is structured information that describes, explains, and/or locates an electronic file. Metadata provides answers to questions like "what is it," "where did it come from," and "who created it?"[5]

Records Retention Schedule: A document that identifies and describes an organization's records, usually at the series level, provides instructions for the disposition of records throughout their life cycle.[6]

Software as a Service (SaaS): Software applications are remotely owned or managed by the provider and are accessible to users through a client, typically the Internet. The user controls neither the underlying infrastructure nor applications. Examples of SaaS applications include web-based email, iCloud©, GoogleDocs™, Dropbox©, and Survey Monkey.™[7]

SSL (Secure socket layer): A type of security or cryptographic protocol used to transmit documents over the internet. SSL encrypts data using a public key, which is known to everyone, and a private key, which is only known to the recipient of the message. These keys ensure that the data is transmitted securely over the internet.

3 Introduction to DocuSign®: Electronic Signature Vendor

[2] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing (Draft),* NIST, January 2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
[3] Uniform Real Property Electronic Recording Act. (2005-391, s. 1.)
[4] ESIGN, Pub.L. 106-229, 14 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch.96
[5] "Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition." North Carolina Department of Cultural Resources, Nov. 2010. Web. <http://www.records.ncdcr.gov/guides/Metadata_Guidelines_%2020101108.pdf>.
[6] "A Glossary of Archival and Records Terminology." Society of American Archivists
[7] "Best Practices for Cloud Computing Records Management Considerations." North Carolina Department of Cultural Resources. August 2012. Web. < http://www.records.ncdcr.gov/guides/cloud_computing_final_20120801.pdf>

The DocuSign® e-Signature Transaction Platform streamlines the process of creating, sending, signing, and completing documents. Additionally, it provides an extensive set of security certifications to safeguard transactions made electronically. This section details some of the basic components of DocuSign® including its SaaS-web platform, security credentials, and capabilities in assuring privacy.

3.1 Software as a Service

DocuSign® uses Software as a Service (SaaS) e-signature authentication program that allows users to work inside one program where documents can be automated, sent, signed, and returned. According to Gartner research, Software as a Service (SaaS) is now the preferred delivery model for digital signatures. SaaS-based offerings will be used for 80% of all new North American e-signature purchases by 2013, compared with 15% in 2009. SaaS provides mobile capabilities and it includes both cloud storage and local server saving capabilities.

3.2 System Requirements

Since DocuSign® uses a SaaS platform, the operating system of both the administrator's and user's computer is not important. Access to the internet is the only requirement for being able to use DocuSign®. The DocuSign® application is rendered via an internet browser. DocuSign® supports most modern web browsers and mobile technologies.

3.3 Security and Privacy

Security Credentials

DocuSign® follows national and international security standards and protocols. It also conforms to the following credentials:

- ISO 27001 certified as an Information Security Management System.
- Third-party audited; SSAE 16 examined and tested annually
- PCI DSS 2.0 compliant to ensure the safe handling of credit cardholder information; secure card data security process
- TRUSTe certified, trusted privacy seal for consumers
- Member US Department of Commerce Safe Harbor; ensures compliance with EU Directive 95/46/EC on the protection of personal data

DocuSign® has a formal Key Management Program and DocuSign® implements a key escrow encryption solution designed to protect sensitive data. Encryption is deployed between the client, Web hosts and servers exchanging sensitive data, including application code.

DocuSign® has implemented Secure Sockets Layer (SSL) 256-bit encryption for transmission and Advanced Encryption Standard (AES) 128-bit encryption for data storage. SSL 256-bit encryption is deployed for transmission of sensitive data over the public Internet and the DocuSign® production environment, and AES 128-bit encryption is implemented to provide additional protection for data storage.

DocuSign® utilize 128-bit SSL encryption to encrypt data stream communications, document exchange, transaction content and signature events through the console from a laptop or workstation, whether internal within an enterprise, outside of an enterprise, over the open internet, or within VPN or tunneled session directly to the database.

The DocuSign® system protects critical elements of customer documents, envelope data, and

signing transaction data in secure document data packets. These document data packets are stored throughout the document signing process. The detailed envelope history, recipient information and routing instructions are stored in the envelope table of the database. Confidential envelope content, including documents, signatures and document form data, are stored in AES 128-bit encrypted data packets. Envelope and encrypted data is tied to a customer account and sending account using unique user identification values. DocuSign® personnel do not have the ability to view encrypted customer documents. This process and actions on customer envelopes are tracked and detailed within DocuSign®'s systematically generated digital audit trail.[8]

For more information on DocuSign® 's credentials, go to:
http://www.DocuSign.com/company/customer-partner-trust

Privacy

If a document will be reviewed by multiple recipients and includes sensitive data such as social security or credit card numbers, DocuSign® allows you to conceal those values. This feature is a data tag called SecureFields. By adding a SecureField data tag, the information will be viewable to the person entering the information, but will be hidden from other signers or recipients. The sensitive information can be retrieved once the envelope is completed and the final recipient downloads the form data.

Although DocuSign® has many security measures in place, it is important to take extra precaution when sending documents via the internet with social security numbers and other personal identifying information. General Statute 132- 1.10 states that a state agency cannot "require an individual to transmit the individual's social security number over the Internet, unless the connection is secure or the social security number is encrypted." Documents sent through the e-signature client will be encrypted; however, every agency should make sure transactions are being made on a secure network especially if there is personal information in the document. The agency must take all precautions necessary to protect private information. Additionally, every agency should give recipients the option to sign on paper if personal information appears on the form.

4 DocuSign® Contract Specifics

4.1 DocuSign® Eligibility and Implementation

The Office of the State Controller contracted DocuSign® to provide the SaaS e-signature technology. The service is available to other state agencies and affiliates. The following groups will be able to subscribe: Executive Branch agencies; Non-State Agencies such as the University of North Carolina University System and member campuses; Instructional components of the Department of Public Instruction; Instructional components of the North Carolina Community College System; and Local and Municipal governments. The Office of the State Controller (OSC) signed a two-year contract with DocuSign® and other agencies can access the services of that contract as they need them. Once an agency determines their needs, the agency will sign a supporting agreement directly with DocuSign®.

[8] "Statewide Electronic Commerce Program" North Carolina Office of State Controller. Web. < http://www.osc.nc.gov/secp/SECP_eForms_Digital_Signatures_Security.html>

DocuSign® should easily integrate into offices 'current technology through the use of standard application programming interfaces (APIs). Additionally, it is integrated with North Carolina Identity Management (NCID)for authentication. Additionally, OSC will work with agencies to create an on-boarding plan and provide assistance in determining level(s) of assurance that may be needed for their business process. OSC and the agency will determine which forms would be easily automated, the priority for applying e-signatures, and the potential back-end integrations. Most forms and processes will be administered by their agencies and tailored to meet their needs.

4.2 Training and Support

DocuSign® will provide initial vendor training and OSC will provide training to agency system administrators. For basic desk support, users can direct general questions to OSC but DocuSign® Account Managers will be available for more complicated issues. Online resources are also listed in *6 DocuSign® Additional Support* of this document.

For in-person training, DocuSign® will host "Technology Days" which will include demonstrations and presentations for participating agencies and groups. "Technology Days" will cover laws, regulations, security and compliance, product overview, benefits, deployments, and any other applicable topics. OSC can be contacted to learn about upcoming "Technology Days."

DocuSign® account manager contact information is located here:
http://www.osc.nc.gov/SECP/SECP_eForms_Digital_Signatures_Contact_Info.html

4.3 Master Service Agreement

OSC's Role and Participating Agencies

OSC signed a Master Service Agreement with DocuSign® that represents all eligible government entities. OSC serves has the contract manager for this agreement and is responsible for developing policies, procedures, and best practices for eforms and digital signatures; administrating the Master Service Agreement; facilitating the enrollment of participants; and general project management and oversight. Each participating agency will sign a supporting agreement with DocuSign®. The entity that enters into a supporting agreement is responsible for paying for the cost of service. Each participating agency will have to execute a Purchase Order with DocuSign®.

Envelope Allowance

OSC selected an Envelope Allowance Subscription. With the Envelope Allowance Subscription, the State is allotted the number of envelopes specified in the order form during any given term. An "envelope" is a transaction with unlimited signers, certified delivery recipients, carbon copy recipients, and attachments. The total number of Envelopes used is based on the sum of all Envelopes that have been sent for signature or for certified delivery from an authorized account. It is important to note that an Envelope is considered used at the time it is sent by an authorized user; regardless if the recipient performs any action on the envelope.

Costs

As noted above, the Master Service Agreement includes a tiered licensing rate based on State volume. Since OSC purchased 100,000 Envelopes per twelve (12) month term, the envelope

allowance subscription rate begins at $0.48 per transaction. This rate decreases based on volume. Agencies may purchase Envelope Allowance Subscriptions at any time during the 24 month period for the balance of the 24 month initial term with provisions for 2 year extensions.
…
The minimum purchase for an Envelope Allowance Subscription is 10,000 envelopes. However, agencies can aggregate purchases with other agencies in order to meet the minimum envelope allowance. The tiered pricing system is listed in the table below.

Envelope Allowance Subscriptions

Total number of Envelopes purchased by the State through all Envelope Allowance Subscriptions over the preceding twelve months; including the Envelope Allowance Subscription purchase by OSC in the initial Purchase Order	Envelope Factor (multiplied by number of Envelopes purchased in each Envelope Allowance Subscription)
10,000 – 49,999	$0.55
50,000 – 99,999	$0.50
100,000 – 249.999	**$0.48**
250,000 – 499,999	$0.475
500,000 – 749,999	$0.46
750,000 – 999,999	$0.45
1,000,000 and above	$0.43

OSC's Envelope Allowance Subscriptions falls into the bolded category above.

Storage

North Carolina has specific laws that dictate cloud computing, however the CIO has exempted this initiative from HB22.[9] Therefore, electronic documents can be saved in DocuSign®'s cloud-based system. DocuSign® provides unlimited storage and hosting of all documents. Its primary data center site is located in Seattle, Washington with a secondary site in Chicago, Illinois. These two sites are hosted by Savvis. Additionally, DocuSign® has a disaster recovery site in Dallas, Texas hosted by SunGuard.

Some agencies may choose to remove their documents from the cloud storage and save their electronic records to a state server. OSC has purchased a State license to DocuSign® Fetch, a tool that allows Agencies to export DocuSign® PDF documents. Fetch will also export the form data into a .csv file that can be opened with Microsoft Excel. There is no additional charge to individual agencies for this feature. Each agency should choose an appropriate and consistent workflow for storing their electronic documents. Take in account retention schedules of specific documents, especially those with long-term values, and any additional applicable laws that might dictate where records can be stored.

See the *Best Practices for Cloud Computing Records Management Considerations* guide for more information on saving documents in the cloud.
http://www.records.ncdcr.gov/guides/cloud_computing_final_20120801.pdf

To access records retention and disposition schedules, please visit: www.records.ncdcr.gov

[9] Session Laws of North Carolina 2011-391 (HB 22).

Additional Services

OSC has negotiated the inclusion of additional services to help agencies fulfill their business and legal needs. DocuSign® and OSC will review these services periodically and engage in conversation making sure all expectations are met. DocuSign® includes the following services:

- *DocuSign® INK*: DocuSign® Ink is an application (app) that that is used to help promote the broad adoption of DocuSign® by allowing users to access and sign documents from any computers, tablets, or smart mobile devices. With DocuSign® Ink, you can place text and check boxes to complete forms, drag–and–drop your legally binding signature into documents, and then return securely via email.
- *eNotary*: DocuSign® is developing a solution for the State's eNotary initiative that will integrate into the current functionality of the DocuSign® multi-tenant platform. This is not a custom development; therefore, there will be no additional development costs. This service will be used according to the Electronic Notary Public Act. For more information visit the Secretary of State's webpage on Electronic Commerce located here: http://www.secretary.state.nc.us/enotary/
- *API*: The DocuSign® API will provide seamless integration of the e-signature system into your agencies' current technology setups. The API is a standard capability for the platform, and will carry no on-going access fees. Each new implementation by a participating agency will require an API certification. However, DocuSign® fully integrates with NCID and new credentials are not required for login.

For additional information on the Master Service Agreement or to read the Agreement click here: http://www.osc.nc.gov/SECP/SECP_eForms_Digital_Signatures.html

5 DocuSign® Account Administration

5.1 Electronic Documents and Envelopes

Documents

DocuSign® allows you to upload an existing document for signatures or to create a new document inside the client software. You can add tags to the document to alert recipients where to fill in extra information and where to sign or initial. If you plan to use the documents over again, you can save an original as a template; thus, allowing you to easily send the document to a new recipient. Additionally, to help manage your document, DocuSign® has a feature called "template matching." Template matching will check to make sure the same document has not been uploaded more than once. Remember to name your templates in a manner that will allow you and others who share the DocuSign® account to find it. By giving the document template an explicit, descriptive name, you will be more efficient as you only have to create or upload the document once.

Envelopes

When you send a document, it gets packaged in a digital envelope. Similar to a paper envelope, you can add more than one electronic document for signature per envelope before sending it to the recipient. An "envelope" can include multiple documents, unlimited signers, certified delivery recipients, carbon copy recipients, and attachments. Within the DocuSign® client, you can search, void, resend, and clone envelopes. You can also update envelopes by

removing or adding documents until one of the signers has completed the process. Additionally, you can view an envelope's status and history at any point in its workflow.

5.2 Managing your documents and envelopes

DocuSign® is flexible in terms of "where" you store your information. First, you can download the completed envelope. DocuSign® will produce a zip file that includes a PDF of the signed document and a summary report with important ancillary information called metadata including time stamps, IP addresses, and security certificates. Once downloaded, you can save the signed document and the summary report to the state server. Choose a naming convention that makes it easy to find the document later and make sure to save the signed document and its respective summary report together. It is recommended that the naming convention you choose clearly indicates which document goes with each respective summary report, since they are downloaded as two separate PDF files. Any document with long-term value needs to be downloaded and saved to a state-owned server.

You can also choose to keep the envelope in the DocuSign® client through DocuSign® Fetch. The DocuSign® console is set up similar to an email client allowing you to create folders in which to save your envelopes. To keep your documents organized, it is important to actively manage your DocuSign® account so that you can find all needed materials at a later time. DCR recommends that you create an electronic folder system to label and organize your documents similar to your paper documents. Organize your documents in a method that is best tailored to your work habits.

The DocuSign® console mimics the look of an email inbox. The default view will show envelopes from the past 30 days.

Searching capabilities through Custom Fields

The sender can create custom fields for envelopes. These fields can add additional information about the envelope that contains documents. More than one document can be inside an envelope, so custom fields for envelopes describe a transaction, not a specific document. Useful envelope information could include a tracking number or descriptive titles based on a specific naming convention. These fields are not seen by the signers.

Recipient Management

The recipient can be given permission to make changes to the envelope including adding recipients; changing routing order; and setting authentication options for other recipients. If recipients are given the ability to make changes; make sure everyone has a consistent model for adding envelope metadata or adding additional signers.

Envelope History

At any point in an envelope status, the sender can view the envelope history. The history will include the security certificate. Changes cannot be made manually to an envelope's history.

5.3 Signing a Document

Guided Signing and Free-Form Signing

DocuSign® has two ways recipients can sign, initial, or add data to a document—guiding signing and free-form signing. The guided signing feature allows the sender to assign tags for signatures, initials, and other information. These tags can be placed directly into a template or

per individual document. DocuSign® Second, the sender can choose to send a free-form signing document. Free-Form Signing allows you to send documents without adding tags. When recipients open free-form signing documents, DocuSign® walks the recipient through an orientation and then the recipient sees the Click & Drag dialog box in the upper left corner of the document window. The recipients will apply their own tags to sign, initial and add other information onto the document in order to complete signing.

Sign On Paper

Signers can print the document and fax it in. However, when the signer signs on paper, they are instructed to fax the document to DocuSign® who will then scan the document and upload it to the client. Users can scan and upload it themselves also. Administrators have the ability to turn this feature off; but General Statute 132-1.10 states that agencies cannot "require an individual to transmit the individual's social security number over the Internet, unless the connection is secure or the social security number is encrypted." So if a document has personal information, users should be allowed to print and sign the document.

Signer Features

The administrator can give the signer different options. The following should be considered when implementing DocuSign® into your current procedures:

- ***Transfer signing responsibility.*** The sender can give signers the ability to transfer signing responsibilities to another person. However, the sender can turn off this option. Before sending a document, determine if the intended signer can re-assign who signs any given document.
- ***Login to DocuSign®.*** Employees with DocuSign® accounts can sign their documents inside the client. You can require that employees sign-in to sign a document.
- ***Send completed document through email.*** You can request that DocuSign® automatically send the completed document to all signers through email. However, the email is not considered secure. Do not use this function if there is sensitive material like social security numbers in the document.

5.4 DocuSign® Account Management

Preset Information

When setting up the account, make sure all the information stored in the client such as the address or logo is correct *(Update your DocuSign® ID card*). This information may be used inside the documents, so it important that it is accurate.

User Groups and Shared Inbox

Administrators can create different user groups. These user groups can then be granted certain permissions inside the system. Additionally, the DocuSign® administrator can give multiple users access to one account. Therefore, the DocuSign® account becomes a shared responsibility of several users who may or may not interact with the documents in the same way. If you share a DocuSign® account with another user, you will need to develop one consistent organization method—decide if you intend to save documents to the state server or keep them in the DocuSign® console. It is important that all parties sharing an account are familiar with the workflow of saving documents and following an agreed upon naming

convention ("Best Practices for File Naming" May, 2008)[10] It is recommended that you choose either to keep all documents saved in the client or all documents saved on the state server to prevent any confusion about the location of the documents.

5.5 Collaboration Tools

Document Markup and Field Markup

Document Markup: Allows signers to make changes to the entire document using features like white out document text, edit text, and new text to existing test, or add text in a blank space. In document markup, the entire document can be changed by the recipients.

Field Markup: The sender can indicate specific document fields that the recipients can edit.

Whoever makes the changes, must initial them in the document; additionally all changes must be approved by the other recipients. If someone has signed the document prior to a change being made, the document will be returned to them for approval. An audit trail of these changes is kept with the document.

Transfer Envelope Custody

The administrator can transfer envelop custody at different points in the document's active life cycle. By creating a rule, the administrator can set who sees the document throughout its various stages. The person who sends the document does not have to be the person who receives the completed form. If your office routinely transfers custody of a document, it is important that the workflow clearly states that the last recipient save the completed document in a manner that is in compliance with public record law.

6 Digital Signature and Electronic Records Management

6.1 Document Retention

Retention rules are set up through the DocuSign® account manager and can be set at the account level. This means that retention rules cannot be set for individual documents or document types by an administrator, making it more difficult to retain documents that have longer retention requirements. Therefore, NCDCR recommends that any document that must be retained for three years or longer be removed from the client and saved on the state server. Additionally, if the state terminates its contract with DocuSign®, remove your documents from cloud storage and save it on a state server.

6.2 Create a Document Workflow

A digital document workflow should be created to show responsibility for a document throughout its life cycle. This workflow must address who is responsible for saving a final copy and respective metadata so that your office is in compliance with public record law and their records retention schedule. Before implementing DocuSign®, create a document workflow and then have all users follow that workflow to ensure that all documents are handled uniformly. The workflow should be easily accessible for all users. See www.records.ncdcr.gov for more information.

[10] North Carolina State Archives, "Best Practices for File Naming." Last modified May, 2008. Accessed October 29, 2012. http://www.records.ncdcr.gov/erecords/filenaming_20080508_final.pdf.

7 DocuSign® Additional Support

For more recent in-depth information on DocuSign®, visit the resources listed below.

DocuSign® Support Site:
https://www.DocuSign.com/support

DocuSign® User Guide:
https://www.DocuSign.com/sites/default/files/DocuSign_Service_User_Guide.pdf

DocuSign® Administration Reference Guide:
https://www.DocuSign.com/sites/default/files/Account%20Administration%20Reference%20Guide.pdf

Free DocuSign® Webinars:
https://www.DocuSign.com/support

eForms and Digital Signatures- Contact Information:
http://www.osc.nc.gov/SECP/SECP_eForms_Digital_Signatures_Contact_Info.html